IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of	
EVRARD et al.	Atty. Ref.: 550-619
Serial No. 10/527,812	Group: 2196
Filed: June 14, 2005	Examiner: K. Vicary

For: PROCESSING ACTIVITY MASKING IN A DATA PROCESSING SYSTEM

* *

January 28, 2008

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

I. REAL PARTY IN INTEREST

The real party in interest in the above-identified appeal is ARM Limited by virtue of an assignment of rights from the inventors to ARM Limited, said assignment recorded June 14, 2005 at Reel 19330, Frame 510.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of
EVRARD et al.
Serial No. 10/527,812
Filed: June 14, 2005

Confirmation No.: 4576
Atty. Ref.: 550-619
Group: 2183
Examiner: K. Vicary

For: PROCESSING ACTIVITY MASKING IN A DATA PROCESSING SYSTEM

* *

APPEAL BRIEF

On Appeal From Group Art Unit 2183

Stanley C. Spooner
NIXON & VANDERHYE P.C.
11th Floor, 901 North Glebe Road
Arlington, Virginia 22203
(703) 816-4028
Attorney for Appellant

TABLE OF CONTENTS

II. RELATED APPEALS AND INTERFERENCES

There are believed to be no related appeals, interferences or judicial proceedings with respect to the present application, other than the Pre-Appeal Brief Request for Review filed September 14, 2007 in this appeal.

III. STATUS OF CLAIMS

Claims 1-10 stand rejected in the outstanding Final Rejection mailed May 14, 2007 (Paper No. 20070507). Claims 1, 2, 5-7 and 10 stand rejected under 35 USC §102 as being anticipated by Qiu (U.S. Patent 6,804,782). Claims 3, 4, 8 and 9 stand rejected under 35 USC §103 as being unpatentable over Qiu in view of Kissell (U.S. Patent 6,625,737). The above rejections of claims 1-10 are appealed.

IV. STATUS OF AMENDMENTS

No further response has been submitted with respect to the Final Official Action in this application other than the filing of a Pre-Appeal Brief Request for Review which decision was mailed on November 29, 2007 (Paper No. 20071126).

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' specification and figures provide an explanation of the claimed invention set out in independent claims 1 and 6, with each claimed structure and method step addressed as to its location in the specification and in the figures.

"1. Apparatus for processing data [processing system 2 shown in Figure 1 and discussed on page 4, line 21 to page 5, line 9 and elsewhere in the specification], said apparatus comprising:

a processor core [processor core 4 shown in Figure 1 and discussed on page 4, line 21 to page 5, line 9 and elsewhere in the specification] operable to execute data processing instructions to generate result data values; and

data processing registers [register bank 12 shown in Figure 1 and discussed on page 4, line 21 to page 5, line 9 and elsewhere in the specification] holding data values defining state of said processor core to which said result data values are written; wherein

at least one data processing instruction [conditional instruction 24 shown in Figure 2 and discussed on page 6, lines 4-33 and elsewhere in the specification] executed by said processor core [4] is a conditional-write data processing instruction encoding condition codes [condition codes 26 shown in Figure 2 and discussed on page 6, lines 4-15 and elsewhere in the specification] specifying conditions under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core [step 34 shown in Figure 3 and discussed at page 6, lines 28-33 and elsewhere in the specification]; and further comprising a trash register [item 51 shown in Figure 1 and discussed on page 7, line 25 to page 8, line 4 and elsewhere in the specification] to which a result data value will be written [step 50 shown in Figure 3 and discussed at page 7, line 25 to page 8, line 4 and elsewhere in the specification] instead of a data processing register upon execution of said conditional-write data processing instruction when said condition codes within said conditional-write data processing instruction do not permit a write to effect a change in state of said processor core [4]."

"6. A method of processing data, said method comprising the steps of:

generating result data values upon execution by a processor core [processor core 4 shown in Figure 1 and discussed on page 4, line 21 to page 5, line 9 and elsewhere in the specification] of data processing instructions, at least one data processing instruction [conditional instruction 24 shown in Figure 2 and discussed on page 6, lines 4-33 and elsewhere in the specification] executed being a conditional-write data processing instruction encoding condition codes [condition codes 26 shown in Figure 2 and discussed on page 6, lines 4-15 and elsewhere in the specification] specifying conditions under which said conditional-write data processing instruction will or will not be permitted [step 34 shown in Figure 3 and discussed at page 6, lines 28-33 and elsewhere in the specification] to write data to effect a change in state of said processor core [4] and wherein a result data value is not written to a data processing register holding a data value defining state of said processor core when condition codes within said condition-write data processing instruction do not permit [step 34 shown in Figure 3 and discussed at page 7, line 28 to page 8, line 4 and elsewhere in the specification] a write to effect a change in state of said processor core but is instead written to a trash register [item 51 shown in Figure 1 and discussed on page 7, line 25 to page 8, line 4 and elsewhere in the specification]."

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2, 5-7 and 10 stand rejected under 35 USC §102 as being anticipated by Qiu (U.S. Patent 6,804,782).

Claims 3, 4, 8 and 9 stand rejected under 35 USC §103 as being unpatentable over Qiu in further view of Kissell (U.S. Patent 6,625,737).

VII. ARGUMENT

Appellants' arguments include the fact that the burden is on the Examiner to first and foremost properly construe the language of the claims to determine what structure and/or method steps are covered by that claim. After proper construction of the claim language, the burden is also on the Examiner to demonstrate where a single reference (in the case of anticipation) or a plurality of references (in the case of an obviousness rejection) teaches each of the structures and/or method steps recited in independent claims 1 and 6.

The Court of Appeals for the Federal Circuit has noted in the case of *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 USPQ 481, 485 (Fed. Cir. 1984) that "[a]nticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim."

Furthermore, the Court of Appeals for the Federal Circuit has stated in the case of *In re Rouffet*, 47 USPQ2d 1453, 1458 (Fed. Cir. 1998)

> to prevent the use of hindsight based on the invention to defeat patentability of the invention, this court **requires** the examiner to show a **motivation** to combine the references that create the case of obviousness. In other words, the Examiner **must show reasons** that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. (Emphasis added).

In its recent decision, the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (April 2007), held that it is often necessary for a court to look to interrelated teachings of multiple patents, the effects of demands known to the design community or present in the marketplace and the background knowledge possessed by a person of ordinary skill in the art in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. The Supreme Court held that "[t]o facilitate review, this analysis should be made explicit." *Id.* at 1396.

The Supreme Court in its *KSR* decision went on to say that it followed the Court of Appeals for the Federal Circuit's advice that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" (the Supreme Court quoting from the Court of Appeals for the Federal Circuit in *In re Kahn*, 78 USPQ2d 1329 (Fed. Cir. 2006)).

A. General differences between the claimed invention and the Qiu reference (U.S. Patent 6,804,782)

The present invention relates to providing data processing systems which manipulate secure data and at the same time maintain a high degree of security (Background of the Invention, specification, page 1).

As discussed in detail in Appellants' previously filed Amendment (filed April 17, 2007, pages 11 and 12), there is a common problem in the present invention and the Qiu patent of preventing the characteristic power consumption signature associated with a write to a data processing register indicating that a write has taken place. However, the two solutions are dramatically different. The Qiu reference solves the problem by masking - an algorithm producing a significant increase in activity within the power signature serves to mask any changes which would occur as a result of the conditional write data processing operation. Qiu's provision of an algorithmic solution for generating masking power usages is a known manner of defeating the so-called simple power analysis (SPA).

The present invention, in writing to the "trash register" represents a significant improvement in security defense and focuses on the intrinsic weaknesses of an encryption algorithm such as in the Qiu patent. Such weaknesses may well be undetectable by way of an SPA and yet may still be detected by using differential power analysis (DPA). The presently claimed invention recognizes that, even on the level of single instructions being executed by a processor core, there is still a detectable change in power usage (detectable using DPA) where data is written to a particular register and where data is not written to a register.

Qiu's attempts to mask this power usage difference is simply a different approach from Applicants' invention which utilizes a "trash register" and writes a result data value to the trash register when the condition codes do not permit a write to effect a change in the processor core. While the Qiu device overcomes a simple power analysis (SPA), it can be defeated by using a differential power analysis (DPA). The presently claimed invention addresses the same problem addressed in Qiu, but not only defeats SPA, but differential power analysis (DPA) as well.

B. Appellants' appealed from independent claims 1 and 6 specifically recites a "trash register" and the Examiner addresses this in the first full paragraph on page 3 of the Official Action

The Examiner fails to identify any structure disclosed in the Qiu reference which comprises the claimed "trash register."

The Examiner's discussion in section 4 on page 5 of the official action does not identify any structure in the Qiu patent which corresponds to the claimed "trash register" of claim 1 or the "writing" step of claim 6. Absent any allegation by the Examiner that Qiu suggests the claimed trash register or the claimed writing step, the failure to allege is taken as an admission that this structure and method step are missing from the Qiu reference.

Accordingly, Qiu cannot anticipate or render obvious the subject matter of independent claims 1 or 6, or claims dependent thereon, under 35 USC §102 because all clamed elements and method steps are not shown in a single reference.

C. In addition to the "trash register," independent claims 1 and 6 also requires that the interconnection such that "a result data value will be written instead of a data processing register upon execution of said conditional-write data processing instruction . . ."

The Examiner has not indicated any interrelationship between the non-identified "trash register" (which he presumably believes is present in Qiu) and the interrelationship specifying that result data values are written to the trash register instead of a data processing register. Because anticipation requires all elements "arranged as in the claim," the anticipation rejection also fails for lack of this claimed interrelationship.

The claim language appears to be controlling and the last paragraph in claim 1 specifies writing the "result data value" to the trash register "when said condition codes within said conditional-write data processing instruction do not permit a write to effect a change in state of said processor core." Thus, depending upon the "conditional-write data processing instruction," the instruction will either write to "a data processing register" or to the claimed "trash register."

The claimed interrelationship between the claimed trash register and the claimed data processing registers is simply not disclosed in the Qiu reference. As a result, there is clearly no support for a rejection of independent claims 1 or 6, or claims dependent, as anticipated by the Qiu reference because Appellants claimed interrelationship is not disclosed.

D. The Examiner fails to appreciate that the Qiu reference teaches away from the claimed invention by requiring an unnecessary mathematical operation

The cryptographic algorithm of Qiu carries out a number of mathematical operations, with the necessity of performing these operations being dependent on values in a private key. Where a particular mathematical operation is not needed, Qiu teaches performing an unnecessary mathematical operation in order to mask the presence or absence of the particular mathematical operation. This is shown in

Qiu's Figure 3 and described at column 4, lines 21-35. It will be appreciated that in the "normal" portion of the cryptographic algorithm (step 300) where mathematical operations are "necessary," the data processing apparatus of Qiu will execute various instructions in order to carry out the algorithm.

As stated in Qiu, "while the algorithm is being implemented" (at column 4, line 27), when it is established that an operation is not required (by checking the key at step 304) an unnecessary mathematical operation and store to memory are performed (steps 308 and 312). The algorithm represented by Figure 3 will involve many distinct instructions being carried out by the data processing apparatus. Therefore, instead of Qiu teaching the claimed subject matter, i.e., directing the result data value to be stored either in a "data processing register" if storage is desired or in the "trash register" if the data is not desired, Qiu merely requires the performance of an algorithm which includes an unnecessary mathematical operation. Qiu simply fails to disclose any concept of a single instruction being executed in one of two different ways as claimed in Appellants' independent claims 1 and 6.

Because Qiu teaches the sufficiency of a different solution to the problem (even though, as noted above, Qiu's solution does not prevent differential power analysis (DPA)), Qiu actually would lead one of ordinary skill in the art away from Appellants' claimed apparatus and the claimed interrelationship between apparatus elements. Because Qiu teaches away from the claimed invention, this evidences the non-obviousness of Appellants' claimed combination and any further rejection of claim 1 or claims dependent thereon is respectfully traversed.

E. The Examiner appears to misunderstand the language of claim 1 with respect to the meaning of the word "instruction"

The Examiner seems to be attempting to interpret the word "instruction" to cover whole sections of algorithmic procedure. This interpretation is inconsistent with the discussion in Qiu, specifically Figures 8 and 10.

Figure 8 illustrates a section of example code, showing how the Qiu algorithm is implemented. Note in particular the steps 7-9 which show what happens when a "0" is encountered in the key (described at column 7, lines 23-29), which is when Qiu teaches performing the unnecessary mathematical operation (see also column 3, lines 55-56 and step 304 of Figure 3).

It will be noted that at step 7, Qiu requires a subroutine MonPro to be called. This subroutine is illustrated in Figure 10 and described at column 7, lines 39-49. This subroutine involves the execution of many instructions.

In light of the known and conventional understanding of the word "instruction" as set out in Appellants' specification and as known to those of ordinary skill, it is clear that Qiu is not concerned with events occurring at the instruction level and rather is concerned with events at the algorithm level.

The Examiner also attempts to consider that a 0 occurring in a private key (which the Examiner considers to be a "condition code") invokes the entire

"MonPro" subroutine in Figure 10. Those having even rudimentary skill in this art would not consider this to be a condition code which is encoded in an instruction to determine how that instruction is to be executed.

While the Examiner appears to be citing various portions of the Qiu reference which he believes disclose the claimed subject matter, a detailed analysis illustrates that the Qiu reference has nothing to do with Appellants' claimed invention. The fact that the Examiner misunderstands and/or misapplies the terms in the claim further evidences the inability of the Examiner to establish a *prima facie* case of either anticipation or obviousness.

F. The Examiner fails to provide any evidentiary support for a rejection of claims 1, 2, 5-7 and 10 under 35 USC §102(e) over the Qiu reference

As noted above in section A, there are substantial and basic differences between the claimed invention and the invention disclosed in the Qiu patent. The subject matter of section A above is herein incorporated by reference.

The Examiner fails to identify any structure in the Qiu reference which comprises the claimed "trash register" as required in section B which is herein incorporated by reference. The Examiner has failed to indicate any teaching in the Qiu reference of the claimed interrelationship between the claimed "trash register" and the writing of a result date value to such a trash register as discussed in section C above, which is also incorporated herein by reference. In addition, as noted in section D above and incorporated by reference, the Examiner appears to improperly interpret the word "instruction" to cover whole sections of algorithmic procedure. This is inconsistent with the disclosure in the Qiu reference.

As noted above, in order to properly support a rejection under 35 USC §102, it is incumbent upon the Examiner to establish where **each and every claimed element** and **each and every claimed interrelationship between elements** are disclosed in a single prior art reference. As noted in sections B, C and E above, the Examiner has failed to identify where the Qiu reference teaches the claimed "trash register," the claimed interrelationship, i.e., the writing of result data values to the trash register instead of a data processing register and the claimed "instruction."

At least one of the claimed elements and interrelationship between claimed elements in independent claims 1 and 6 is missing in the Qiu reference and therefore no *prima facie* case of rejection based upon "anticipation" of claims 1 and 6 over the Qiu reference is made out.

G. The Examiner fails to provide any evidentiary support for a rejection of claims 3, 4, 8 and 9 under 35 USC §103 as unpatentable over Qiu in view of Kissell

As noted above in section F, the Examiner has failed to indicate how or where the Qiu reference teaches at least one claimed element (the "trash register" or the "instruction") and at least one claimed interrelationship (writing a result data value to a "trash register" instead of a data processing register). Because the above-mentioned B and C clearly establish both a claimed structure and a claimed interrelationship which is simply missing from the Qiu reference, both the claimed structure and the claimed interrelationship must be disclosed somewhere in the Kissell reference in order to support a rejection under 35 USC §103.

Appellants have reviewed the Examiner's arguments under sections 10 and 11 in the Final Rejection and can find no allegation that Kissell teaches the "trash register" or the interrelationship missing from the Qiu reference. Thus, even if the Examiner combines the Qiu and Kissell references, that combination does not disclose either Appellants' claimed "trash register" or claimed interrelationship involving writing a result data value to the trash register. Accordingly, there can be no *prima facie* basis for a rejection of independent claims 1 and 6 or any claims dependent thereon over the Qiu/Kissell combination.

The Examiner fails to provide any "reason" or "motivation" for combining the Qiu and Kissell references. As required by the U.S. Supreme Court's holding in *KSR* noted above, the Examiner's analysis as to any apparent reason or motivation for combining elements "should be made explicit." The Examiner has failed to set out any "explicit" rationale.

The only discussion in the Final Rejection regarding a motivation for combining the Qiu and Kissell references are in sections 10 and 11. This discussion merely concludes that it would be obvious to use "Kissell's teaching to save power" and "that the teaching of Kissell fits into the environment of Qiu." Neither of these statements comprises an explicit analysis of the Examiner's reason or motivation alleging that it would be obvious to combine these two references.

As adopted in the Supreme Court's in the *KSR* decision, the Court of Appeals for the Federal Circuit has consistently held that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." Here, the Examiner merely provides a conclusory statement that it would be obvious to combine the references and fails to provide any articulated reasoning with any rational underpinning to support the conclusion of obviousness.

As a result of the above, the Examiner has failed to establish a *prima facie* case of obviousness because he has failed to meet the required burden of establishing some factual basis for the combination of the two references. Accordingly, any rejection of claims 1 and 6 and claims dependent thereon as being obvious over the Qiu/Kissell combination is respectfully traversed.

Finally, as noted in section D above, the Examiner apparently fails to appreciate that the Qiu reference teaches away from the claimed invention by instead requiring an unnecessary mathematical operation. The Court of Appeals for the Federal Circuit has held that it is "error to find obviousness where references ‘diverge from and teach away from the invention at hand’.” *In re Fine*, 5 USPQ2d 1596, 1599 (Fed. Cir. 1988). Because, as confirmed in section D above, Qiu teaches away from the claimed invention, any *prima facie* case of obviousness has been clearly rebutted by the Appellants.

Accordingly, any future allegation that independent claims 1 and 6 or claims dependent thereon are obvious under 35 USC §103 is respectfully traversed.

VIII. CONCLUSION

Based upon the Final Rejection, it is not clear that the Examiner understands the prior art or the claimed invention. There is no basis for an anticipation or obvious rejection where the primary reference Qiu fails to teach at least one claimed element (the “trash register”) and at least one claimed interrelationship between elements (moving the data value to either the processor register or the trash register). Accordingly, there is no basis for a §102 anticipation rejection. The defects in the Qiu reference are not cured by the Kissell patent and there is no reason to combine these references. Accordingly, there is no *prima facie* basis for a §103 obviousness rejection. Therefore, no Additionally, the Examiner seems to ignore the fact that Qiu teaches away from the claimed invention and thus would rebut any *prima facie* case, even if one were made.

As a result of the above, there is simply no support for the rejections of Appellants' independent claims or claims dependent thereon under 35 USC §102 or §103. Thus, and in view of the above, the rejection of claims 1-10 under 35 USC §§102 and 103 is clearly in error and reversal thereof by this Honorable Board is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: ______________________________
Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
Enclosure

IX. CLAIMS APPENDIX

1. Apparatus for processing data, said apparatus comprising:

a processor core operable to execute data processing instructions to generate result data values; and

data processing registers holding data values defining state of said processor core to which said result data values are written; wherein

at least one data processing instruction executed by said processor core is a conditional-write data processing instruction encoding condition codes specifying conditions under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core; and further comprising

a trash register to which a result data value will be written instead of a data processing register upon execution of said conditional-write data processing instruction when said condition codes within said conditional-write data processing instruction do not permit a write to effect a change in state of said processor core.

2. Apparatus as claimed in claim 1, comprising a register bank having a plurality of data registers to which result data values are written.

3. Apparatus as claimed in claim 1, wherein writing to said trash register is programmably disabled by a trash register control signal.

4. Apparatus as claimed in claim 3, wherein said trash register control signal is stored in a system configuration register.

5. Apparatus as claimed in claim 2, wherein said trash register is part of said register bank, said trash register being unmapped to a register number such that said trash register may not be specified by a register specifying operand value.

6. A method of processing data, said method comprising the steps of:

generating result data values upon execution by a processor core of data processing instructions, at least one data processing instruction executed being a conditional-write data processing instruction encoding condition codes specifying conditions under which said conditional-write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core and wherein

a result data value is not written to a data processing register holding a data value defining state of said processor core when condition codes within said condition-write data processing instruction do not permit a write to effect a change in state of said processor core but is instead written to a trash register.

7. A method as claimed in claim 6, wherein said data processing register is part of a register bank having a plurality of data registers to which result data values are written.

8. A method as claimed in claim 6, wherein writing to said trash register is programmable disabled by a trash register control signal.

9. A method as claimed in claim 8, wherein said trash register control signal is stored in a system configuration register.

10. A method as claimed in claim 7, wherein said trash register is part of said register bank, said trash register being unmapped to a register number such that said trash register may not be specified by a register specifying operand value.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.